

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION	:	
OF THE UNITED STATES OF AMERICA	:	CASE NO. 1:15-ES-4
FOR AN ORDER AUTHORIZING THE	:	
INTERCEPTION OF ELECTRONIC	:	UNDER SEAL
COMMUNICATIONS	:	

ATTACHMENT A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

FILED

2015 FEB 20 A 8:39

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF ELECTRONIC
COMMUNICATIONS

CASE NO. 15-cr-00015-RLV-DCK
CLERK OF DISTRICT COURT
ALEXANDRIA, VIRGINIA
UNDER SEAL

**APPLICATION FOR AN ORDER AUTHORIZING INTERCEPTION OF
ELECTRONIC COMMUNICATIONS**

The United States of America, by and through Assistant United States Attorney Whitney Dougherty Russell and Trial Attorney Michael Grant (hereinafter "the prosecutors"), hereby applies to the Court pursuant to Section 2518 of Title 18, United States Code, for an Order authorizing the interception of electronic communications. In support of this application, counsel states the following:

1. The prosecutors are investigative or law enforcement officers of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, attorneys authorized by law to prosecute or participate in the prosecution of offenses enumerated in Section 2516(1)(c) of Title 18, United States Code.

2. A copy of the memorandum of an official specially designated by the Attorney General of the United States authorizing this application is attached to this application as Exhibit A.

3. This application is for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications of [REDACTED] and other unidentified administrators and users ("TARGET SUBJECTS") of the child pornography website upf45jv3bziuctml.onion ("TARGET WEBSITE") occurring

over the private message function ("TARGET FACILITY 1") and private chat function ("TARGET FACILITY 2"), of the TARGET WEBSITE, concerning offenses enumerated in Section 2516 of Title 18, United States Code.

4. The prosecutors have discussed the circumstances of the above offenses with Special Agent Caliope Bletsis of the Federal Bureau of Investigation, who has participated in the conduct of this investigation, and have examined the affidavit of Special Agent Bletsis, which is attached as Exhibit B to this application and is incorporated herein by reference. Based upon that affidavit, your applicants state upon information and belief that:

a. there is probable cause to believe that the TARGET SUBJECTS have committed, are committing, and will continue to commit violations of the following offenses:

- i. 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise;
- ii. 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography;
- iii. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution and Conspiracy to Receive and Distribute Child Pornography;
- iv. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography; and

b. there is probable cause that the TARGET SUBJECTS, during the period of interception authorized by this Order, will use TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the "TARGET FACILITIES"), in furtherance of the offenses described above;

c. There is probable cause to believe that the interception of electronic

communications of the TARGET SUBJECTS over the TARGET FACILITIES will reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the target offenses; in addition, these electronic communications are expected to constitute admissible evidence of the commission of the above-described offenses. It is expected that monitoring of the electronic communications of the TARGET SUBJECTS over the TARGET FACILITIES, if authorized, will provide valuable evidence against the TARGET SUBJECTS and others currently unknown to law enforcement involved in illegal activities that cannot reasonably be obtained by other means; and

d. It has been established as detailed in the attached Affidavit that normal investigative procedures have been tried and have failed, reasonably appear unlikely to succeed if tried, or are too dangerous to employ.

5. There are no previous applications which are known to have been made to any judge of competent jurisdiction for approval of the interception of the oral, wire or electronic communications of any of the same individuals, facilities, or premises specified in this Application, except as set forth in the affidavit.

6. This Court has territorial jurisdiction to issue the requested order under 18 U.S.C. § 2518(3) because the computer server intercepting all communications and on which the TARGET WEBSITE, including the TARGET FACILITIES, are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception.

WHEREFORE, there is probable cause to believe that the TARGET SUBJECTS are engaged in the commission of offenses involving violations of Title 18, United States Code, Sections 2251 and 2252A, and that during the period of interception applied for herein, the TARGET SUBJECTS will use the TARGET FACILITIES to communicate with each other and with others as yet unknown, in connection with the commission of the above-described offenses. The prosecutors also believe that, if the interception herein applied for is authorized by this Court, electronic communications of the TARGET SUBJECTS concerning those offenses will be intercepted.

7. On the basis of the allegations contained in this application, which in turn is based on the attached affidavit of Special Agent Bletsis:

IT IS HEREBY REQUESTED that this Court issue an order pursuant to the power conferred upon it by Section 2518 of Title 18, United States Code, authorizing FBI and/or individuals employed by or operating under a contract with the government and acting under the supervision of the FBI, to intercept electronic communications of the TARGET SUBJECTS, occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing

the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the receipt and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; (5) the location and identity of computers used to further the target offenses; and (6) admissible evidence of the commission of the above-described offenses - or for a period of thirty (30) days, to be measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the Order or 10 days after the Order is entered, whichever is earlier from the date of this authorization.

IT IS FURTHER REQUESTED that this Court direct that its Order be executed as soon as practicable after it is signed and that all monitoring of electronic communications shall be conducted in accordance with Chapter 119 of Title 18, United States Code, as outlined in Agent Bletsis's affidavit. That is, the computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to a facility in [REDACTED] MD, where certain FBI personnel will be stationed while the TARGET WEBSITE remains operating. Each private message and private chat will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed

by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chats will be sealed with the court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

IT IS FURTHER REQUESTED that the prosecutors or any other Assistant United States Attorney or Department of Justice Trial Attorney familiar with the facts of this case, shall cause to be provided to the Court a report on or about the fifteenth and thirtieth day following the date of the Order or the date interception begins, whichever is later, showing the progress that has been made toward achievement of the authorized objectives and the need for continued interception, although if the Order is renewed for a further period of interception, the application for renewal may serve as the report on or about the thirtieth day. If any of the above-ordered reports should become due on a weekend or holiday, such report shall become due on the next business day thereafter.

IT IS FURTHER REQUESTED that the Court direct that the Court's Order, as well as the supporting Application, Affidavit (along with its attachments), proposed

Orders, and all interim reports filed with the Court, be sealed until further order of this Court, except that copies of the Order, in full or redacted form, may be served on FBI agents as necessary to effectuate the Court's Order. Moreover, the Government hereby requests authorization to disclose the existence of the Interception Order and the contents of pertinent collected electronic communications, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as appropriate for the purposes of providing relevant facts to a Court in support of any complaints, arrest warrants or search warrants. In addition, the Government requests authorization to disclose facts, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as necessary to provide relevant testimony at any preliminary hearings, detention hearings, grand jury proceedings and other proceedings pertaining to the TARGET SUBJECTS and others as yet unknown. The Government also requests authorization to disclose facts to foreign investigative or law enforcement officers, pursuant to Title 18, United States Code, Section 2517(7), as necessary to the proper performance of the official duties of the officer making or receiving such disclosure, and that foreign investigative or law enforcement officers may use or disclose such facts or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

IT IS FURTHER REQUESTED that no inventory or return of the results of the foregoing interception need be made, other than the above required reports, before 90 days from the date of the expiration of the Order, or any extension of the Order, or at such time as the Court in its discretion may require.

IT IS FURTHER REQUESTED that, upon an ex parte showing of good cause to a judge of competent jurisdiction, the service of the above inventory or return may be

postponed for a further reasonable period of time.

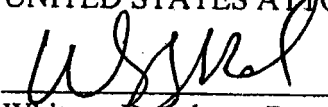
I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED in Alexandria, Virginia, on February 20, 2015.

Respectfully submitted,

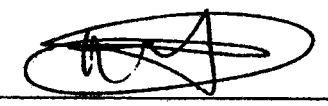
DANA J. BOENTE
UNITED STATES ATTORNEY

By:


Whitney Dougherty Russell
Assistant United States Attorney

DAMON KING
ACTING CHIEF
Child Exploitation and Obscenity Section
Criminal Division
U.S. Department of Justice

By:


Michael Grant
Trial Attorney

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

ALEXANDRIA DIVISION

IN THE MATTER OF THE APPLICATION	:	
OF THE UNITED STATES OF AMERICA	:	CASE NO. 1:15-ES-4
FOR AN ORDER AUTHORIZING THE	:	
INTERCEPTION OF ELECTRONIC	:	UNDER SEAL
COMMUNICATIONS	:	

EXHIBIT A



Office of the Attorney General
Washington, D.C.

ORDER NO. 3055-2009

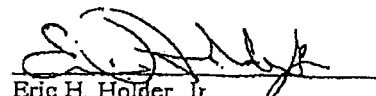
SPECIAL DESIGNATION OF CERTAIN OFFICIALS OF THE CRIMINAL DIVISION AND
NATIONAL SECURITY DIVISION TO AUTHORIZE APPLICATIONS FOR COURT
ORDERS FOR INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS

By virtue of the authority vested in me as the Attorney General, including 28 U.S.C. § 510, 5 U.S.C. § 301, and 18 U.S.C. § 2516(1), and in order to preclude any contention that the designations by the prior Attorney General have lapsed, the following officials are hereby specially designated to exercise the power conferred by section 2516(1) of title 18, United States Code, to authorize applications to a Federal judge of competent jurisdiction for orders authorizing or approving the interception of wire and oral communications by the Federal Bureau of Investigation or a Federal agency having responsibility for the investigation of the offense(s) as to which such application is made; when such interception may provide evidence of any of the offenses specified in section 2516 of title 18, United States Code:

1. The Assistant Attorney General in charge of the Criminal Division, any Acting Assistant Attorney General in charge of the Criminal Division, any Deputy Assistant Attorney General of the Criminal Division, and any Acting Deputy Assistant Attorney General of the Criminal Division;
2. The Assistant Attorney General for National Security, any Acting Assistant Attorney General for National Security, any Deputy Assistant Attorney General for National Security, and any Acting Deputy Assistant Attorney General for National Security, with respect to those matters delegated to the supervision and responsibility of the Assistant Attorney General for National Security. These officials of the National Security Division shall exercise this authority through, and in full coordination with, the Office of Enforcement Operations within the Criminal Division.

Attorney General Order No. 2943-2008 of January 22, 2008, is revoked effective at 11:59 p.m. of the day following the date of this order.

2-26-09
Date


Eric H. Holder, Jr.
Attorney General



U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

The Honorable Dana J. Boente
United States Attorney
Eastern District of Virginia
Alexandria, Virginia

FEB 18 2015

Attention: Keith Becker and Michael Grant,
Trial Attorneys, U.S. Department of Justice,
Criminal Division, Child Exploitation and
Obscenity Section

Dear Mr. Boente:

An appropriate official hereby approves an application to be made to a federal judge of competent jurisdiction for an order under Section 2518 of Title 18, United States Code, authorizing, for a thirty (30) day period, the interception of electronic communications occurring over the private message function and private chat function of the website "upf45jv3bziuctml.onion," in connection with an investigation into possible violations of federal felonies by Steven W. Chase, and others as yet unknown.


The above-described application may be made by you or any other attorney on your staff who is an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code.

Sincerely,

Leslie R. Caldwell
Assistant Attorney General
Criminal Division

FEB 18 2015

Date


KENNETH A. BLANCO
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

FILED

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

2015 FEB 20 A 8:42

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF ELECTRONIC
COMMUNICATIONS

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA
CASE NO. 1:15-ES-4

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR AN ORDER
AUTHORIZING INTERCEPTION OF ELECTRONIC COMMUNICATIONS**

I, Caliope Bletsis, being duly sworn, state the following:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation (FBI) since December 2004, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am

empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. This affidavit is submitted in support of the Government's Application for an Order under Title 18, United States Code, Section 2518, authorizing the interception, for a period of up to thirty days, of the electronic communications of [REDACTED] and other unidentified administrators and users ("TARGET SUBJECTS") of a child pornography website upf45jv3bziuctml.onion, hereinafter the "TARGET WEBSITE,"¹ occurring over the private message function ("TARGET FACILITY 1") and private chat function ("TARGET FACILITY 2"), of the TARGET WEBSITE.

3. As a result of my personal participation in this investigation, through information obtained from other federal and foreign law enforcement agents and witnesses, including physical surveillance and the review of documents, and on the basis of other information that I have reviewed and determined to be reliable, I allege facts to show that:

- a. There is probable cause to believe that the TARGET SUBJECTS have committed, are committing, and will continue to commit offenses specified in Title 18, United States Code, § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography, and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Knowing Possession of, Access or Attempted Access With Intent to View

¹ The actual name of TARGET WEBSITE is known to law enforcement. The site remains active and disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "TARGET WEBSITE".

Child Pornography (collectively, the "TARGET OFFENSES").

- b. There is probable cause to believe that particular electronic communications of TARGET SUBJECTS concerning the TARGET OFFENSES will be obtained through interception of electronic communications occurring over TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the "TARGET FACILITIES"). In particular, these communications are expected to lead to the revelation of evidence concerning the TARGET OFFENSES, including the content of communications between and among the TARGET SUBJECTS. In addition, these electronic communications are expected to constitute admissible evidence of the commission of the TARGET OFFENSES.

4. The requested Order is sought for a period of time until the interception fully reveals the manner in which the TARGET SUBJECTS and their confederates participate in the TARGET OFFENSES, or for a period of thirty (30) days, whichever occurs first, pursuant to Title 18, United States Code, Section 2518(5). Pursuant to Section 2518(5) of Title 18, United States Code, it is further requested that the 30-day period be measured from the earlier of the date on which investigative or law enforcement officers begin to conduct interception under this Court's Order or 10 days from the date of this Court's Order.

5. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/employees/computer

forensic professionals; and my experience, training and background as a Special Agent with the FBI.

6. Because this affidavit is being submitted for the limited purpose of securing authorization for the collection of electronic communications, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for an order authorizing the interception of electronic communications occurring over the Internet via communications occurring over TARGET FACILITY 1 and TARGET FACILITY 2.

RELEVANT STATUTES

7. This investigation concerns alleged violations of: Title 18, United States Code, § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Knowing Possession of, Access or Attempted Access With Intent to View Child Pornography.

- a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, *inter alia*, federal child pornography crimes listed in Title 18, Chapter 110, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;
- b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly making, printing or publishing, or causing to be made, printed or published, or conspiring to make,

print or publish, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

- c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly receiving or distributing, or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and
- d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DESCRIPTION OF TARGET FACILITIES

- 8. TARGET FACILITY 1: The private message function of the TARGET WEBSITE is similar to e-mail messages and allows the TARGET SUBJECTS to send and

receive communications with other users and/or administrator(s) of the TARGET WEBSITE, such that the private message is only accessible to the user who sent or received such a message and the site administrator(s).

9. TARGET FACILITY 2: The private chat function of the TARGET WEBSITE allows the TARGET SUBJECTS to communicate in real-time directly with each other and the communications are only visible and accessible to the users engaged in the private chat and the administrator(s).

10. Other than TARGET FACILITY 1 and TARGET FACILITY 2, described above, there are no other private areas of the TARGET WEBSITE where communications are only visible to some, but not all, registered users.

TARGET SUBJECTS

11. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] all other current users and administrators of the TARGET WEBSITE remain unidentified.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

12. The following definitions apply to this Affidavit:

- a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a

bulletin board may post messages in reply to a post. A message “thread,” often labeled a “topic,” refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through “private messages.”

Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the site administrator.

- b. “Child erotica,” as used herein, means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
- c. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- d. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such

device.”

- e. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.
- f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It

commonly includes programs to run operating systems, applications, and utilities.

- h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- j. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the

Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- m. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the Internet Service Provider (“ISP”) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- n. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- o. A “Proxy Server” is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. Proxy

servers can facilitate access to content on the World Wide Web and prove anonymity.

- p. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- q. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
- r. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- s. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up

Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

SUMMARY OF PROBABLE CAUSE

13. The TARGET SUBJECTS are the administrators and users of the TARGET WEBSITE who regularly send and receive illegal child pornography via the TARGET WEBSITE which operates as a “hidden services” located on the Tor network, further described below. This TARGET WEBSITE is dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes such as the TARGET OFFENSES. As of February 12, 2015, a law enforcement agent visited the TARGET WEBSITE, in an undercover capacity, and confirmed that the site remains active, accessible and substantially the same as described herein.

The Tor Network

14. The TARGET WEBSITE operates on an anonymity network available to Internet users known as “The Onion Router” or “Tor” network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user’s web browser or by downloading the free “Tor browser bundle” available at www.torproject.org.²

² Users may also access the Tor network through so-called “gateways” on the open Internet such as “onion.to” and “tor2web.org,” however, use of those gateways does not provide users with the anonymizing benefits of the Tor

15. Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server.

16. Tor also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Tor network itself, entire websites can be set up as "hidden services." Hidden services, like other websites, are hosted on computer servers that communicate through IP addresses and operate in the same manner as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dfiku7f" followed by the suffix ".onion." A user can only reach these hidden services if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor hidden service. Neither law enforcement nor users can therefore determine the location of the computer that

network.

hosts the website through those public lookups.

Finding and Accessing the TARGET WEBSITE

17. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of the TARGET WEBSITE on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the TARGET WEBSITE as well as the site's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography, including the TARGET WEBSITE. Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by a user, making it extremely unlikely that any user could simply stumble upon the website without understanding its purpose and content. In addition, upon arrival at the TARGET WEBSITE, the user sees images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses the TARGET WEBSITE has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of TARGET WEBSITE Content and Criminal Use of the TARGET

FACILITIES

18. Between September 16, 2014 and February 3, 2015, FBI Special Agents, acting in an undercover capacity, connected to the Internet via the Tor Browser and accessed TARGET WEBSITE.³ The TARGET WEBSITE is a message board website whose primary purpose is the

³ As of February 18, 2015, the URL of the TARGET WEBSITE had changed from muff7i44irws3mwu.onion to upf45jv3bziuctml.onion. I am aware from my training and experience that it is possible for a website to be moved

advertisement and distribution of child pornography. According to statistics posted on the site, TARGET WEBSITE contained a total of 95,148 posts, 9,333 total topics, and 158,094 total members. Based on the earliest known post, the website appeared to have been operating since approximately August 19, 2014.

19. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to TARGET WEBSITE; and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

20. Upon accessing the "register an account" hyperlink, the following message was displayed:

"VERY IMPORTANT. READ ALL OF THIS PLEASE.

I will add to this as needed.

from one URL to another without altering its content or functionality. I am also aware from the instant investigation that the administrator of the TARGET WEBSITE periodically changes the location and URL of the TARGET WEBSITE in order to avoid law enforcement detection. An FBI agent accessed the TARGET WEBSITE in an undercover capacity on February 18, 2015, at its new URL, and determined that its content has not changed.

The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.

After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.

Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.

Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.

The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing or Tor we also recomend that you turn off javascript and disable sending of the 'referer' header."

21. After accepting the above terms, registration to the message board then requires a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above. After successfully registering and logging into the site, the following sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observed:

<u>Section – Forum</u>	<u>Topics</u>	<u>Posts</u>
General Category		
[TARGET WEBSITE] information and rules	25	236
How to	133	863
Security & Technology discussion	281	2,035
Request	650	2,487
General Discussion	1,390	13,918
The INDEXES	10	119
Trash Pen	87	1,273

[TARGET WEBSITE] Chan		
Jailbait ⁴ – Boy	58	154
Jailbait – Girl	271	2,334
Preteen – Boy	32	257
Preteen – Girl	264	3,763
Jailbait Videos		
Girls	643	8,282
Boys	34	183
Jailbait Photos		
Girls	339	2,590
Boys	6	39
Pre-teen Videos		
Girls HC ⁵	1,427	20,992
Girls SC/NN	514	5,635
Boys HC	87	1,256
Boys SC/NN	48	193
Pre-teen Photos		
Girls HC	433	5,314
Girls SC/NN	486	4,902
Boys HC	38	330
Boys SC/NN	31	135
Webcams		
Girls	133	2,423
Boys	5	12
Potpourri		
Family [TARGET WEBSITE] – Incest	76	1,718
Toddlers	106	1,336
Artwork	58	314
Kinky Fetish		
Bondage	16	222
Chubby	27	309
Feet	30	218
Panties, nylons, spandex	30	369
Peeing	101	865
Scat	17	232

⁴ Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors.

⁵ Based on my training and experience, I know that the following abbreviations respectively mean: HC – hardcore, i.e., depictions of penetrative sexually explicit conduct; SC – softcore, i.e., depictions of non-penetrative sexually explicit conduct; NN – non-nude, i.e., depictions of subjects who are fully or partially clothed.

Spanking	28	251
Vintage	84	878
Voyeur	37	454
Zoo	25	222
Other Languages		
Italiano	34	1,277
Portugues	69	905
Deutsch	66	570
Espanol	168	1,614
Nederlands	18	264
Pyccknn – Russian	8	239
Stories		
Fiction	99	505
Non-fiction	122	675

22. An additional section and forum was also listed in which members could exchange usernames on a Tor-network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children. Another service available to users was the ability to send private chat messages between users.

23. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The last post section included the date and time of the post as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

24. A review of the various topics within the “[TARGET WEBSITE] information and

rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

25. A review of topics within the remaining forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography and child erotica of prepubescent females, males, and toddlers. Examples of these are as follows:

On February 3, 2015, the user “[REDACTED]” posted a topic entitled “[REDACTED]” in the forum “Pre-teen – Videos - Girls HC” that contained numerous images depicting a prepubescent or early pubescent female engaged in sexually explicit conduct. One of these images depicted the female being orally penetrated by the penis of a naked male.

On January 30, 2015, the user “[REDACTED]” posted a topic entitled “[REDACTED]” in the forum “Pre-teen Photos – Girls HC” that contained hundreds of images depicting a prepubescent female engaged in sexually explicit conduct. One of these images depicted the female being orally penetrated by the penis of a male.

On September 16, 2014, the user “[REDACTED]” posted a topic entitled “[REDACTED]” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting a prepubescent female engaged in sexually explicit conduct and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent female. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

26. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. Analysis of available historical data seized from the TARGET WEBSITE, as described below, revealed that on average over 1,500 unique users visited the website daily and over 11,000 unique users visited the website over the course of a week. A private message feature, TARGET FACILITY 1, also appeared to be available on the site, after registering, that allowed users to send other users private messages,

referred to as "personal messages" or "PMs," which are only accessible to the sender and recipient of the message. Review of the site demonstrated that the site administrator made a posting on January 28, 2015, in response to another user in which he stated, among other things, "Yes PMs should now be fixed. As far as a limit, I have not deleted one yet and I have a few hundred there now...."

27. Further review revealed numerous additional posts referencing private messages or PMs regarding posts related to child pornography, including one posted by a user stating, "Yes i can help if you are a teen boy and want to fuck your little sister. write me a private message."

28. Additionally, law enforcement agents reviewed hundreds of private messages occurring over TARGET FACILITY 1 that were in furtherance of the TARGET OFFENSES and/or provided information on the identities of the TARGET SUBJECTS. These private messages were collected over the server for the TARGET WEBSITE, and law enforcement was able to access these messages through the server copy that was obtained from the search warrant for the TARGET WEBSITE in January 2015. Examples of these messages, which law enforcement believes discusses the sexual abuse of minors, are as follows:

- a. On January 10, 2015, the user [REDACTED] sent a private message to the user [REDACTED] stating: "Hi, thnx! She is cute and tasty indeed...She's arround 1,5yo on that photo....I play with her everytime I have her alone, started from arround 3/4 mo...She's now 3,5. I also have another niece, also 3,5 but they are not sisters, and as tasty as the other one ;-) Never had them together at once unfortunately! I only tried anal once with the niece in my avatar when she was 2,5, almost got the head of my cock inside.... Never penetrated their pussies (except with my tongue) and

never cummed inside their asses or pussies directly (all too dangerous) For the rest, I did everything...Even thought a couple of times to show them on my webcam, naked etc, but never got to do that..."

- b. On January 6, 2015, user [REDACTED] sent a private message to [REDACTED] that contained the following: "My personal feelings are that were you to have a consensual sexual relationship with a child that she enjoyed, two things might make her regret it in her late teens and early twenties. One is the knowledge that her sexual partner was her father and two, the sex was recorded. My name [REDACTED] alludes to my 1080p HD hidden camera glasses I have for recording purposes although I plan to use them with another little girl in my life, a 5 year old brunette pixie not related to me by blood. POV porn is another favorite of mine. ;)."
- c. On December 16, 2014, the user [REDACTED] sent a private message to the user [REDACTED] stating the following: "but contact me only if you are ready to rape your sisters. when you think they are too good for you then don't waste my time!"

29. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private message function of the TARGET WEBSITE site, described above as TARGET FACILITY 1, is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of the TARGET SUBJECTS.

30. The TARGET WEBSITE also includes a feature referred to as "[TARGET WEBSITE] Image Hosting." This feature of the TARGET WEBSITE allows users of the TARGET WEBSITE to upload images of child pornography that are in turn, only accessible to users of the TARGET WEBSITE. On February 12, 2015, an FBI agent operating in an

undercover capacity accessed a post on the TARGET WEBSITE titled [REDACTED] which was created by the TARGET WEBSITE user [REDACTED]. The post contained links to images stored on "[TARGET WEBSITE] Image Hosting". The images depicted a prepubescent female in various states of undress. Some images were focused on the nude genitals of a prepubescent female. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent female.

31. The TARGET WEBSITE also includes a feature referred to as "[TARGET WEBSITE] File Hosting." This feature of TARGET WEBSITE allows users of TARGET WEBSITE to upload videos of child pornography that are in turn, only accessible to users of TARGET WEBSITE. On February 12, 2015, an FBI Agent operating in an undercover capacity accessed a post on the TARGET WEBSITE titled [REDACTED] which was created by the TARGET WEBSITE user [REDACTED]. The post contained a link to a video file stored on "[TARGET WEBSITE] File Hosting." The video depicted an adult male masturbating and ejaculating into the mouth of a nude, prepubescent female.

32. The TARGET WEBSITE also includes a feature referred to as "[TARGET WEBSITE] Chat." On February 6, 2015, an FBI Special Agent accessed "[TARGET WEBSITE] Chat" which was hosted on the same URL as the TARGET WEBSITE. The hyperlink to access "[TARGET WEBSITE] Chat" was located on the main index page of the TARGET WEBSITE. After logging in to [TARGET WEBSITE] Chat, more than 50 users were observed to be logged in to the service. While logged in to [TARGET WEBSITE] Chat, the following observations were made:

- a. User [REDACTED] posted a link to an image that depicted four females performing oral sex on each other. At least two of the females depicted were prepubescent.

- b. User [REDACTED] posted a link to an image that depicted a prepubescent female with an amber colored object inserted into her vagina.
- c. User [REDACTED] posted a link to an image that depicted two prepubescent females laying on a bed with their legs in the air exposing their genitals.
- d. Other images that appeared to depict child pornography were also observed.

33. The images described above, as well as other images, were captured and are maintained as evidence.

34. Messages posted in [TARGET WEBSITE] Chat are generally public and available for all users to see. A review of [TARGET WEBSITE] Chat showed that it also contained a feature allowing users of [TARGET WEBSITE] Chat to send messages privately, over TARGET FACILITY 2, which are only visible to the sender and intended recipient(s). Examples of messages sent using TARGET FACILITY 2 were collected over the server for the TARGET WEBSITE, and law enforcement was able to access these messages through the server copy that was obtained from the search warrant for the TARGET WEBSITE in January 2015. Examples of these messages, which law enforcement believes discusses the sexual abuse of minors, are as follows:

- a. On January 14, 2015, the user [REDACTED] sent a private chat message to [REDACTED] stating "made it easier when daughter comes over...sis still calls me when she gets drunk...of course shes 20 now....still a good fuck ;)."
- b. On January 14, 2015, the user [REDACTED] sent a private chat message to [REDACTED] that stated "mmmm I want to cover that in cum." Prior to this message, [REDACTED] had sent [REDACTED] multiple private chat messages that contained links to images located on hidden services with the path

[REDACTED] after the address. The links were no longer active, but based on my training and experience, I know members of sites such as the TARGET WEBSITE often send links to images of child pornography. The links often expire after a certain amount of time or the original uploader deletes the file.

- c. On January 14, 2015, the user [REDACTED] sent two private chat messages to [REDACTED] that stated "gotta love the internet meet like minded folks" and "alone man but another pedo helped me get started with her."

35. Based on my training and experience and the review of the site by law enforcement agents, I believe that the private chat function of the site, described above as the TARGET FACILITY 2, is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of the TARGET SUBJECTS.

36. A review of message threads also revealed that users discussed traveling to foreign countries with the intent to sexually abuse children in a foreign country. One example of this type of discussion is where user [REDACTED] posted a thread on October 8, 2014, titled "Travel Advice in Asia, SE Asia, and Australia," and asked "I need to take a vacation soon somewhere in Asia or Southeast Asia (though possibly as far as Australia). Can anyone give me some tips for the best places to go to find accessible girls (10-13) in the region?...Whatever I need to know to find some girls for a few days...Pay to play is fine." Another user, [REDACTED] responded on October 8, 2014, and stated, "[Y]ou can try philippines, don't go to Indonesia." A second user, [REDACTED] responded on October 11, 2014, and stated "[Y]ou will find that in most countries child brothels are in the small villages and towns, not in cities...Most brothels will let the very young do BJs, but no fucking which is left with the older girls. In Asian countries, a

child brothel is quite easy to find, just ask around...Best is to arrange a girl to be delivered to your hotel.”

Target Website Sub-Forums

37. While the entirety of the TARGET WEBSITE is dedicated to child pornography, the following sub-forums of the TARGET WEBSITE were reviewed and determined to contain the most egregious examples of child pornography and/or dedicated to textual descriptions of sexually abusing children: (a) Pre-teen Videos - Girls HC; (b) Pre-teen Videos - Boys HC; (c) Pre-teen Photos - Girls HC; (d) Pre-teen Photos - Boys HC; (e) Potpourri – Toddlers; (f) Potpourri - Family Play Pen – Incest; (g) Spanking; (h) Kinky Fetish – Bondage; (I) Peeing; (j) Scat⁶; (k) Stories - Non-Fiction; (l) Zoo; (m) Webcams – Girls; and (n) Webcams – Boys.

Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE

38. In December of 2014, a foreign law enforcement agency advised the FBI that it suspected IP address 192.198.81.106, which is a United States-based IP address, to be associated with the TARGET WEBSITE. A publicly available website provided information that the IP Address 192.198.81.106 was owned by [REDACTED] a server hosting company headquartered at [REDACTED]. Through further investigation, FBI verified that TARGET WEBSITE was hosted from the previously referenced IP address. [REDACTED]

[REDACTED]

[REDACTED] A Search Warrant was obtained and executed at [REDACTED] in January 2015 and a copy of the server (hereinafter the "Target Server") that was assigned IP Address

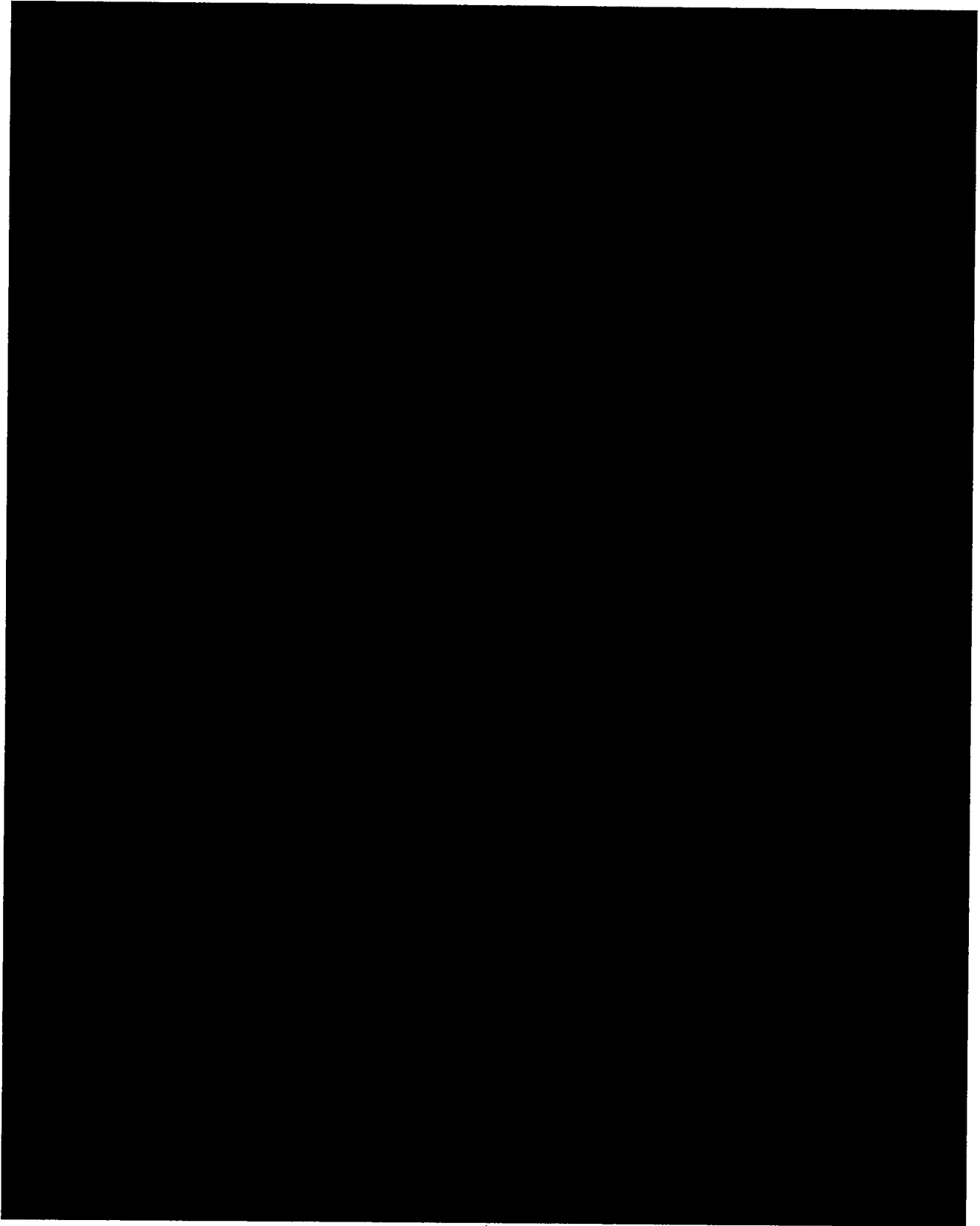
⁶ Based on my training and experience, “scat” refers to sexually explicit activity involving defecation and/or feces.

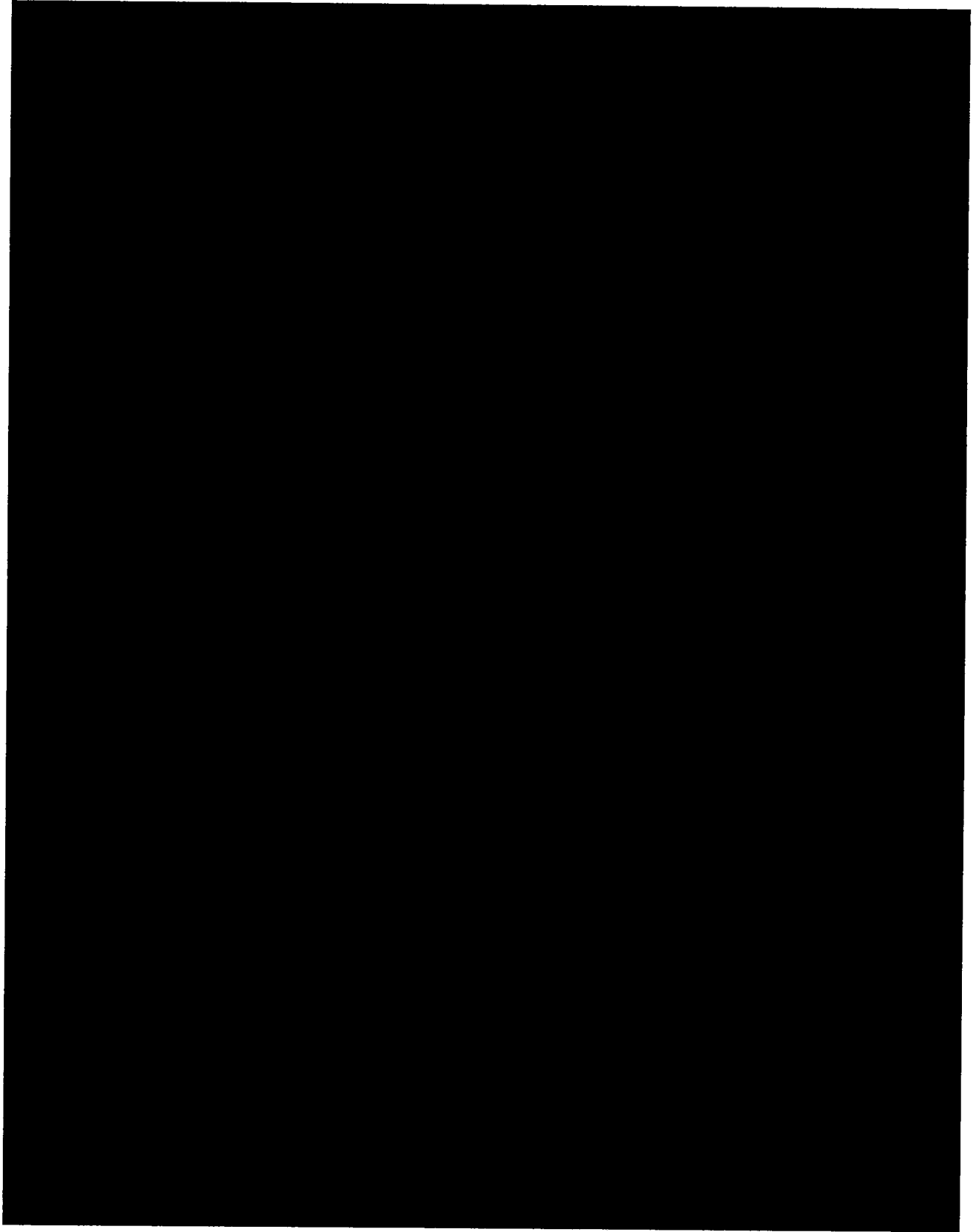
[REDACTED] FBI Agents reviewed the contents of the Target Server and observed that it contained a copy of the TARGET WEBSITE. A copy of the Target Server is currently located on a computer server at a government facility in Newington, VA, in the Eastern District of Virginia.

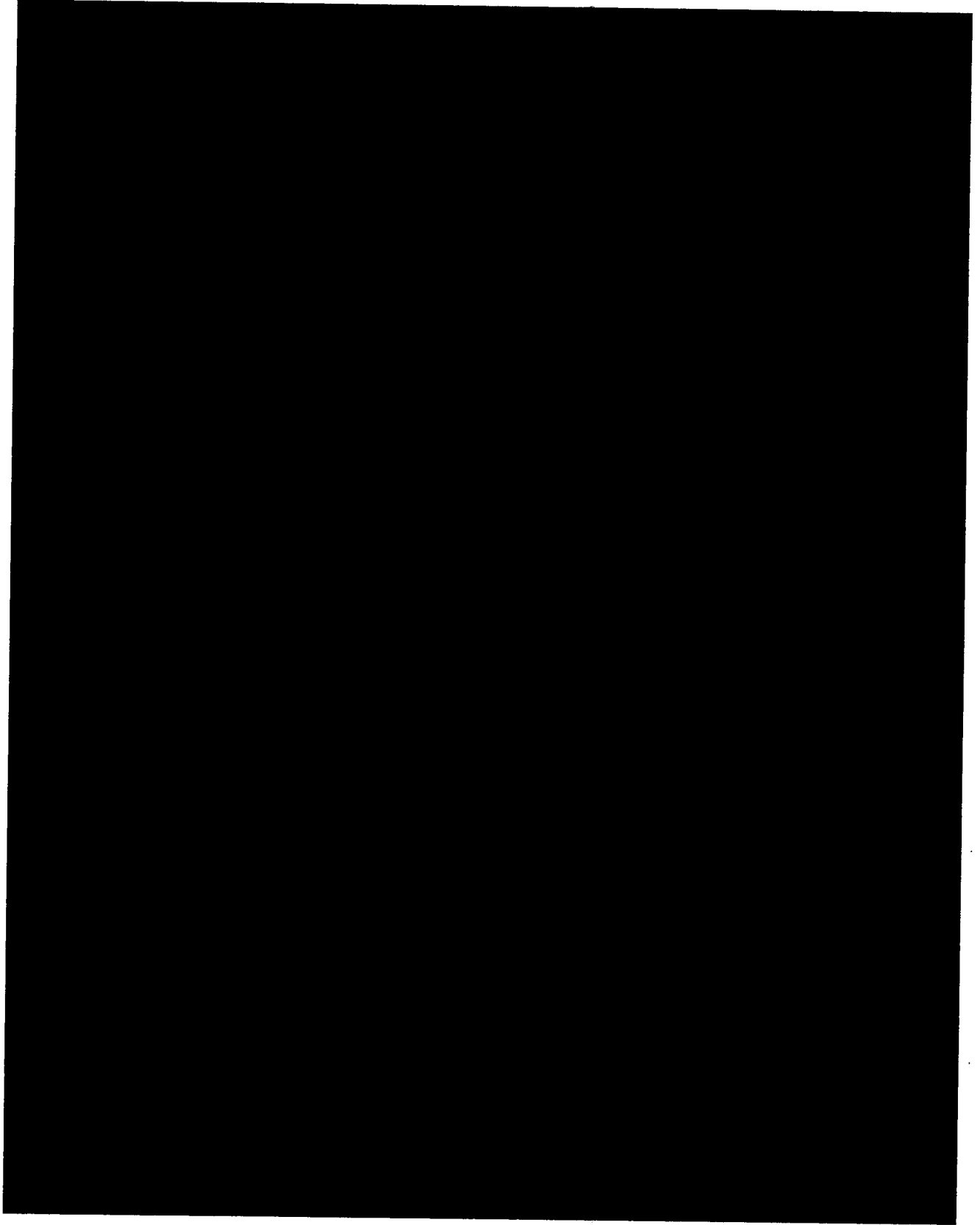
39. While possession of the server data will provide important evidence concerning the criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the administrators and users of TARGET WEBSITE will remain unknown. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of TARGET WEBSITE, the logs of member activity will contain only the IP addresses of Tor "exit nodes" utilized by board users. Those IP address logs cannot be used to locate and identify the administrators and users of TARGET WEBSITE.


[REDACTED]

[REDACTED]





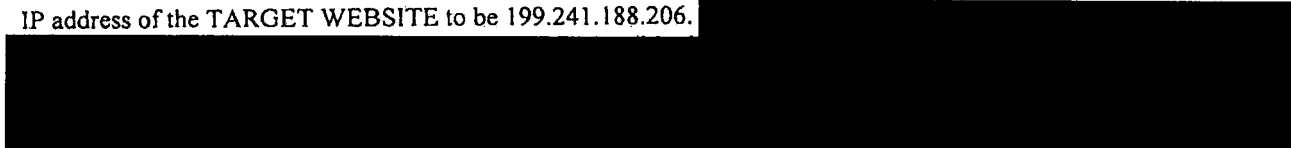




52. Accordingly, on February 19, 2015, FBI personnel executed a court-authorized search at the Naples, FL, residence of the suspected administrator of the TARGET WEBSITE. That individual was apprehended and the FBI has assumed administrative control of the TARGET WEBSITE. The TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia, on which a copy of TARGET WEBSITE currently resides. These actions will take place for a limited period of time, not to exceed 30 days, in order to locate and identify the administrators and users of TARGET WEBSITE through the deployment of the network investigative technique described below. Such a tactic is necessary in order to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.

DEPLOYMENT OF NETWORK INVESTIGATIVE TECHNIQUE

⁷ As explained supra, footnote 3, the administrator of the TARGET WEBSITE periodically changes its location and URL in order to avoid law enforcement detection. As of February 18, 2015, investigation has revealed the current IP address of the TARGET WEBSITE to be 199.241.188.206.



53. As noted above, the TARGET WEBSITE will operate from a government facility in Newington, Virginia, within the Eastern District of Virginia, and remain online and accessible to the TARGET SUBJECTS for a limited period of time. During the period of this authorization, FBI expects to concurrently deploy a court-authorized Network Investigative Technique ("NIT") on the TARGET WEBSITE in an attempt to identify the actual IP addresses and other identifying information for computers used by TARGET SUBJECTS to access the TARGET WEBSITE. The NIT will send one or more communications to TARGET SUBJECTS that access the TARGET WEBSITE after the date of its deployment, which communications are designed to cause the computer receiving it to deliver data that will help identify the computer, its location, other information about the computer, and the user of the computer accessing the TARGET WEBSITE. In particular, the NIT is designed to reveal to the government the computer's actual IP address, the date and time that the NIT determines what that IP address is, a unique session identifier to distinguish the data from that of other computers and other information, and other information that may assist in identifying computers that accesses the TARGET WEBSITE and their users. Separate authorization will be sought from this Court for the execution of that search warrant and the deployment of the NIT.

TARGET SUBJECTS COMMUNICATIONS ON THE TARGET WEBSITE

54. TARGET SUBJECTS can communicate on the TARGET WEBSITE in four ways: (1) through postings or reply postings on the website, which may include videos, images, or links to videos or images, which are visible and accessible to any user who accesses the board, including law enforcement agents; (2) through the public chat feature of the website, which may also include videos, images, or links to videos or images, which are visible and accessible to any user who accesses the board, including law enforcement agents; (3) through TARGET

FACILITY 2, the private chat feature on the website, which is similar to the public chat function but is only visible and accessible to the users engaged in the private chat; and (4) through TARGET FACILITY 1, the private message function, which is similar to e-mail messages and which are only accessible to the user who sent or received such a message and the site administrator(s). Other than the private messaging function and private chat function, there are no private areas of the TARGET WEBSITE where communications are only visible to some, but not all, registered users.

55. In order to access any of the content of the TARGET WEBSITE, it is necessary to register with a username and a password. Only users of the TARGET WEBSITE who register with a username and a password have access to the private messaging and private chat functions. The private message function is not an "instant messaging" system where users communicate in real time, but rather operates similar to sending and receiving e-mails. The private chat function is similar to an "instant messaging" system where the users communicate in real time, but only with other users who are engaged in the private chat. Multiple examples of public postings on the TARGET WEBSITE where TARGET SUBJECTS discuss the use of private messaging and private chat are described herein.

56. TARGET SUBJECTS communicate anonymously on the sites, using aliases known as "screen names." TARGET SUBJECTS rarely, if ever, post any personally identifiable information that would allow law enforcement to identify the TARGET SUBJECTS or the TARGET SUBJECTS actual location on areas of the TARGET WEBSITE accessible to all users. In fact, the site specifically cautions its users not to post or share any identifying information as described in the rules of TARGET WEBSITE listed in paragraph 20 of this affidavit. Based upon my training and experience, users are more likely to send information that

is identifying or that could corroborate other identifying information in private messages or private chats exchanged only between board users. For example, [REDACTED]

[REDACTED]

[REDACTED] Reviewing private messages, private chats, and postings in private areas of the TARGET WEBSITE in real time will allow agents to act upon any identifying details or details about child victims immediately upon the sending or receipt of such a message or chat, rather than waiting for the later execution of a search warrant to retrieve historical private message or private chat data. That information received in real time can be paired with information gathered via the NIT and other information available in postings to help to identify or corroborate the identity of TARGET SUBJECTS. Also based upon my training and experience, users often privately trade child pornography which is facilitated by communication via private messages or private chat. Users may directly send child pornography via private message or private chat, or exchange information that allows them to trade child pornography via other digital platforms – for example, another e-mail account, a file hosting website, or other child pornography websites. Child pornography that is trafficked via file uploading websites is often made available only for a limited period of time, which is a security measure by the user in order to avoid detection. Where law enforcement agents are able to intercept a communication directing a user to a file sharing website or to download location, that

file can be downloaded by law enforcement and therefore preserved as evidence. Accordingly, reviewing such messages in real time may provide crucial evidence of child pornography trafficking which would not be available by reviewing historical messages. Furthermore, I am aware from training and experience as well as the review of seized data from the TARGET WEBSITE that the administrators and moderators of the website communicate with each other regarding the administration, management and facilitation of the TARGET WEBSITE via private messaging. During the period of time that the TARGET WEBSITE will operate from a government facility, those administrators and moderators may communicate via private messages or private chats regarding any changes made to the TARGET WEBSITE and the potential of law enforcement infiltration of the site. Law enforcement agents will be able, following the apprehension of [REDACTED] to communicate as the main administrator of the TARGET WEBSITE. However, law enforcement would not be able, absent the interception of private messages, to learn in real time about communications between other administrators and moderators suggesting an awareness of changes made to the TARGET WEBSITE (to facilitate the investigative techniques discussed herein) and potential actions those administrators and moderators may take to alert others, obstruct justice or destroy evidence. While the TARGET WEBSITE is operating at a government facility for a limited period of time, FBI will have access to all users' private messages and private chats, which may include videos, images, or links to videos or images, which are visible and accessible only to certain users of the sites.

PERSONS LIKELY TO BE INTERCEPTED

57. The INTERCEPTTEES include [REDACTED] and those TARGET SUBJECTS who send or receive private messages or private chats on the TARGET WEBSITE during the 30-day period of this authorization. At this time, because of the anonymous nature of the Tor

network and the choice of the TARGET SUBJECTS to utilize that functionality, the actual identities of the TARGET SUBJECTS are unknown.

NECESSITY FOR COLLECTION OF PRIVATE MESSAGES AND PRIVATE CHATS

58. Based on my training and experience as a Special Agent, as well as the experience of other law enforcement officers involved in this investigation, and based upon all of the facts set forth herein, it is my belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception of electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES as applied for herein, is the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the identity of the TARGET SUBJECTS and that they are engaging in the TARGET OFFENSES. I believe that such combination of investigative steps are the only available technique likely to provide law enforcement with the critical information needed for this investigation, i.e., evidence of the actual identity of the TARGET SUBJECTS and that of their accomplices, aiders and abettors, co-conspirators and participants in illegal activities, who have deployed advanced technology to remain anonymous while conducting their illegal activity; the nature, extent and methods of operation of TARGET SUBJECTS' unlawful activities; the existence and locations of records relating to those activities; communications between TARGET SUBJECTS and their accomplices, aiders and abettors, co-conspirators and participants in those illegal activities; and the location and identity of computers used to further the TARGET OFFENSES.

59. The interception of private messages and private chats in real time is necessary for several reasons. TARGET SUBJECTS communicate anonymously on the sites, using aliases

known as "screen names." As described above, private messaging and private chat is only available to users who register with a username and password. TARGET SUBJECTS rarely, if ever, post any personally identifiable information that would allow law enforcement to identify the TARGET SUBJECTS or the TARGET SUBJECTS actual location on areas of the TARGET WEBSITE accessible to all users. In my training and experience, users are more likely to send information that is identifying or that could corroborate other identifying information in private messages and private chats exchanged only between board users or within private areas only accessible to certain users. For example, [REDACTED]

[REDACTED]

[REDACTED] Reviewing private messages and private chats in real time will allow agents to act upon any identifying details or details about child victims immediately upon the sending or receipt of such a message, rather than waiting for the later execution of a search warrant to retrieve historical private message and private chat data. That information received in real time can be paired with information gathered via the NIT and other information available in postings to help to identify or corroborate the identity of TARGET SUBJECTS.

60. Interception of private messages and private chats is also necessary for the identification and protection of potential victims of child sexual abuse. There are postings to the TARGET WEBSITE by at least two members who contend to have access to children, one of which has posted images that the user contends are of sexual abuse the user has committed against children. That individual ("CD-1") was identified through other investigative means and

admitted to producing images of child pornography subsequent to his arrest [REDACTED] In the event that a user shares information about child sexual abuse and/or the production of child pornography in a private message or private chat that is being monitored in real time, agents can, in conjunction with the deployment of the NIT and any other available evidence, immediately take action to locate and identify that user in an attempt to prevent further abuse of that child. In that scenario, reviewing such private messages and private chats only after the execution of a search warrant would waste crucial time.

61. Moreover, in order for the NIT to have a chance to work, members need to continue to access the TARGET WEBSITE after the NIT is deployed. In order to ensure that users continue to access the TARGET WEBSITE, it is necessary that there be as minimal an interruption as possible in the operation of the TARGET WEBSITE, so as not to create suspicion among the TARGET SUBJECTS that a law enforcement action is taking place on the board. In my training and experience and in reviewing messages posted on the TARGET WEBSITE, and other child pornography and exploitation websites operating on the Tor network, interruptions in service for more than a minimal time period is a tip-off to board users that law enforcement infiltration may be going on and may result in users not accessing the board for a period of time. Law enforcement will review historical private messages and private chats for any identifying information shared by TARGET SUBJECTS, however, that review takes time. Review of the seized copy of TARGET WEBSITE has included [REDACTED]

[REDACTED]

[REDACTED] Analysis of that data is ongoing and efforts are being made to determine which, if any, of the identified [REDACTED] can be utilized to obtain a true identity for any users of TARGET WEBSITE. Other than [REDACTED] and CD 1, none of

the other administrators or users have been identified. Waiting for such a review to be complete before deploying a NIT and monitoring private messages and private chats on the TARGET WEBSITE in real time would deprive law enforcement of potentially crucial information at a critical phase in the investigation.

NORMAL INVESTIGATIVE PROCEDURES

62. Based upon your affiant's training and experience, as well as the experience of other FBI agents and law enforcement officers with whom I have investigated this case, and based upon all of the facts set forth herein, it is your affiant's belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception of electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES is the only available technique with a reasonable likelihood of securing the evidence necessary to prove that the TARGET SUBJECTS are engaging in the SUBJECT OFFENSES beyond a reasonable doubt. Due to the unique nature of the information sought, numerous investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed, reasonably appear to be unlikely to succeed if they are tried, or are too dangerous to employ for the reasons discussed below.

UNAVAILABILITY OF ALTERNATIVE INVESTIGATIVE TECHNIQUES

63. Your affiant and other investigators in criminal investigations of violations of Title 18, United States Code, Sections 2251 and 2252A, et seq., customarily use the following investigative techniques: (a) physical surveillance; (b) use of Grand Jury Subpoenas; (c) interview of subjects or associates; (d) search warrants; (e) infiltration by undercover officers; and (f) use of cooperating individuals.

64. Over the past three years, investigators have also explored various means and methods of investigating Tor based websites and offenders using Tor. As set forth below these techniques are insufficient to accomplish the objectives of the investigation.

Physical Surveillance

65. Physical Surveillance is unavailable because the TARGET SUBJECTS, other than [REDACTED] are unidentified and communicating in a way that provides for their anonymity.

Grand Jury Subpoenas

66. Grand Jury subpoenas are unavailable because all of the TARGET SUBJECTS, other than [REDACTED] are unidentified and communicating in a way that provides for their anonymity.

Interview of Subject or Associates

67. Interviewing TARGET SUBJECTS or any associates is impossible because all of the TARGET SUBJECTS (but for [REDACTED] and CD-1) are unidentified and communicating in a way that provides for their anonymity.

68. CD-1, a member of TARGET WEBSITE previously referenced in this affidavit, who was arrested [REDACTED] was interviewed subsequent to his arrest. He did not provide any information that could be used by law enforcement to identify other users of TARGET WEBSITE.

Search Warrants

69. Search warrants are being used actively in this investigation. For example, FBI expects to execute search warrants to deploy a NIT to attempt to identify the TARGET SUBJECTS. As noted herein, however, the execution of the search warrant to seize a copy of the TARGET WEBSITE was insufficient to identify TARGET SUBJECTS and interdict their illegal activity. While possession of the data will provide important evidence concerning the

criminal activity that has occurred on the server and the TARGET WEBSITE, the identities of the other administrators and users of the TARGET WEBSITE will remain unknown. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of the TARGET WEBSITE, logs of member activity, if any, will contain only the IP addresses of Tor "exit nodes" utilized by board users. Those IP address logs cannot be used to locate and identify TARGET SUBJECTS of the TARGET WEBSITE. In order to attempt to identify those users, the website needs to remain operating so that authorization may be obtained to employ a NIT on the site to identify true IP addresses of TARGET SUBJECTS. The execution of a search warrant to seize the TARGET WEBSITE alone would not provide such authority.

70. Agents could execute another search warrant at a later date to again review historical private messages and private chats by TARGET SUBJECTS. Reviewing only historical private messages, private chats, and postings, however, is not sufficient for the reasons stated above. A search warrant will not provide real-time information about TARGET SUBJECTS or communications between and among the TARGET SUBJECTS about their unlawful activities. That real-time information can be paired with other identifying data from a NIT to allow agents to quickly locate and apprehend TARGET SUBJECTS before or as soon as possible after the TARGET WEBSITE ceases operating. When the TARGET WEBSITE ceases to operate, in my training and experience, there is likely to be speculation among TARGET SUBJECTS that a law enforcement action has been taken against the TARGET WEBSITE. That may cause TARGET SUBJECTS to flee or destroy evidence before they can be apprehended. The need for real-time information that can be quickly acted upon is heightened in the event that TARGET SUBJECTS disclose information about ongoing sexual abuse of child victims. Solely reviewing historical private messages, private chats, or postings may prevent agents from

immediately acting upon evidence of ongoing abuse disclosed via private messages or private chats.

71. Search warrants for the physical premises of the TARGET SUBJECTS are unavailable because the other TARGET SUBJECTS are unidentified and communicating in a way that provides for their anonymity. It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside, or where they receive, hide, transfer, and conceal the proceeds of their crime. Once other TARGET SUBJECTS have been identified, the use of search warrants of physical premises may be a valuable tool. However, until that time, the use of search warrants of physical premises of the TARGET SUBJECTS is infeasible.

72. Agents have considered seizing the TARGET WEBSITE and removing it from existence immediately and permanently. However, at this time, no TARGET SUBJECTS besides the administrator described above have been identified. There are multiple TARGET SUBJECTS who claim that they are sexually abusing children and sharing images of that abuse with others. Removing the TARGET WEBSITE from existence immediately and permanently upon seizure would end the distribution and receipt of child pornography taking place on the TARGET WEBSITE, however, it would prevent law enforcement from attempting to locate and identify the TARGET SUBJECTS and their child victims, and attempting to rescue those child victims from ongoing abuse. Any attempt to identify TARGET SUBJECTS requires that the TARGET WEBSITE remain operating for some period of time. Accordingly, it is your affiant's belief that the seizure of the TARGET WEBSITE in conjunction with its continued operation for a limited period of time, the deployment of a NIT to attempt to identify actual IP addresses used by the TARGET SUBJECTS, and the interception and collection of private messages and private chats sent/received by TARGET SUBJECTS is appropriate in this case.

Confidential Informants, Cooperating Sources, and Undercover Agents

73. Undercover agents have been used in this investigation to access the TARGET WEBSITE and document the sites, their categories, and postings on the sites. Cooperating individuals are unavailable because the TARGET SUBJECTS are currently unidentified and therefore not available to assist with law enforcement activities. The use of undercover agents, confidential informants and cooperating sources in this investigation is unlikely to succeed, however, in terms of meeting the stated objectives of the investigation at this stage. In order to obtain personally identifying data about a TARGET SUBJECT, an undercover agent or cooperating individual would have to engage in private messaging with that TARGET SUBJECT, develop a significant and trusting relationship with the TARGET SUBJECT, and attempt to elicit personally identifying information from the TARGET SUBJECT. As noted above, postings on the TARGET WEBSITE caution its members against providing such information. In my training and experience, such information is much more likely to have been exchanged between existing TARGET SUBJECTS who have already developed such a relationship with each other and shared such information via private messages or private chats.

74. Moreover, using an "administrator" account on the TARGET WEBSITE to attempt to elicit personally identifiable information from TARGET SUBJECTS is not feasible and would immediately be viewed by TARGET SUBJECTS as suspicious and indicative of law enforcement infiltration of the board. That would likely lead unidentified TARGET SUBJECTS to flee the board and/or destroy evidence of their unlawful activity.

Pen Registers and Trap and Trace Devices

75. Pen registers and trap and trace type data have been utilized in this case to verify that the IP Address hosting the TARGET WEBSITE is sending and receiving data on the Tor network. However, at this stage of the investigation, they are inadequate investigative

techniques. Pen registers do not enable law enforcement officers to obtain the content of communications, which is necessary in order to identify the TARGET SUBJECTS. Moreover, because of the way that Tor operates, a pen register and trap and trace device deployed on the TARGET WEBSITE would reveal only the Tor "exit node" used by TARGET SUBJECTS to access the board, which cannot be used to locate and identify that user.

Electronic Interception

76. There have been no prior electronic interceptions of communications occurring on the TARGET WEBSITE.

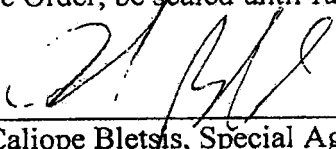
MINIMIZATION

77. Only electronic communications (i.e., private messages and private chats) will be intercepted. All intercepted communications of the TARGET SUBJECTS will be minimized in accordance with Chapter 119 of Title 18, United States Code. The computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to an FBI facility in [REDACTED] Maryland, where certain FBI personnel will be stationed while the TARGET WEBSITE remains operating. Each private message and private chat will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and

secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chats will be sealed with the court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

78. As of February 12, 2015, a search of the Electronic Surveillance (ELSUR) Automated Records Systems for DEA, ICE and the FBI was conducted and revealed no prior applications for Court authorization to intercept the wire, oral, or electronic communications involving the same subjects, facilities, or premises specified in this affidavit.

79. IT IS REQUESTED that this Affidavit, the attached Application, the resulting Order, and all reports submitted pursuant to the Order, be sealed until further order of the court.



Caliope Bletsis, Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me

on this 20 day of February, 2015.



UNITED STATES DISTRICT JUDGE
EASTERN DISTRICT OF VIRGINIA

Anthony J. Trega
United States District Judge

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

2015 FEB 20 A 8:38

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE
INTERCEPTION OF ELECTRONIC
COMMUNICATIONS

CASE NO. 15-1-00015-RLV-DCK
UNDER SEAL
DISTRICT COURT
ALEXANDRIA, VIRGINIA

**ORDER AUTHORIZING INTERCEPTION OF ELECTRONIC
COMMUNICATIONS**

Application under oath having been made before me by Assistant United States Attorney for the Eastern District of Virginia Whitney Dougherty Russell and Department of Justice Child Exploitation and Obscenity Section Trial Attorney Michael Grant (hereinafter "the prosecutors"), who are investigative or law enforcement officers of the United States within the meaning of Section 2510(7) of Title 18, United States Code, for an order pursuant to Section 2518 of Title 18, United States Code, authorizing the interception of electronic communications, and full consideration having been given to the matters set forth therein, the Court finds:

a. there is probable cause to believe that [REDACTED] and other unidentified administrators and users ("TARGET SUBJECTS") of the child pornography website upf45jv3bziuctml.onion ("TARGET WEBSITE") have committed, are committing, and will continue to commit federal felony offenses as provided for by Section 2516(3) of Title 18, United States Code, that is: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; 18 U.S.C. §§ 2252A(a)(5)(B) and

(b)(2), and Knowing Possession of, Access or Attempted Access With Intent to View Child Pornography ("TARGET OFFENSES");

b. there is probable cause that the TARGET SUBJECTS, during the period of interception authorized by this Order, will use the private message function ("TARGET FACILITY 1") and private chat function ("TARGET FACILITY 2"), of the TARGET WEBSITE in furtherance of the offenses described above;

c. there is probable cause to believe that the interception of electronic communications authorized by the Order will reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the TARGET OFFENSES. In addition, these electronic communications are expected to constitute admissible evidence of the commission of the above-described offenses. It is expected that monitoring of TARGET FACILITY 1 and TARGET FACILITY 2 (together referred to as the "TARGET FACILITIES") will provide valuable evidence against the TARGET SUBJECTS involved in illegal activities that cannot reasonably be obtained by other means; and

d. it has been established that normal investigative procedures have been tried and have failed, reasonably appear unlikely to succeed if tried, or are too dangerous to employ.

WHEREFORE, IT IS HEREBY ORDERED pursuant to Section 2518 of Title 18, United

States Code, that the FBI and/or individuals employed by or operating under a contract with the government and acting under the supervision of the FBI, are authorized to intercept electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: (1) the nature, extent and methods of operation of the TARGET SUBJECTS' unlawful activities; (2) the identity of the TARGET SUBJECTS and their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities, or information that may be useful in establishing the identity of their victims, accomplices, aiders and abettors, co-conspirators and participants in their illegal activities; (3) the advertising, receipt, and distribution of child pornography related to those activities; (4) the existence and locations of records relating to those activities; and (5) the location and identity of computers used to further the target offenses; and (6) admissible evidence of the commission of the above-described offenses - or for a period of thirty (30) days, to be measured from the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the Order or 10 days after the Order is entered, whichever is earlier from the date of this authorization.

IT IS FURTHER ORDERED that, pursuant to Section 2518 of Title 18, United States Code, special agents with the FBI, and other "investigative and law enforcement officers," as defined in Section 2510(7) of Title 18, United States Code, to be assisted, if necessary, by authorized translators, are authorized to intercept and to record electronic communications of the TARGET SUBJECTS over the TARGET FACILITIES, and that this Order shall be executed as soon as practicable.

IT IS FURTHER ORDERED that all monitoring of electronic communications shall

be conducted in accordance with Chapter 119 of Title 18, United States Code. That is, the computer server intercepting all communications and on which the TARGET FACILITIES are located will be in Newington, VA, in the Eastern District of Virginia during the period of interception. A copy of intercepted communications will be sent to a facility in [REDACTED] MD, where certain FBI personnel will be stationed while the TARGET WEBSITES remain operating. Each private message will be reviewed over a secure system, and based on the identities of the sender and recipient and the content of the private message or private chat, monitoring personnel will determine as soon as practicable after interception whether the private message or private chat appears to be relevant to the investigation or otherwise criminal in nature. If the private message or private chat is not criminal in nature, the private message or private chat will be marked "minimized" and not accessed by other members of the investigative team. If the private message or private chat appears to be privileged, it will be marked "privileged" and secured from access by other members of the investigative team. If a private message or private chat appears to be relevant to the investigation or otherwise criminal in nature, it will be marked "non-minimized" and may be shared with the other agents and monitors involved in the investigation. If a private message or private chat is marked "minimized" or "privileged," it will not be disseminated to members of the investigative team. All intercepted private messages and private chat will be sealed with the Court upon the expiration of the court's order authorizing the interception. It is anticipated that the monitoring location will be staffed at all times, at which time intercepted communications will be monitored and read. The monitoring location will be kept secured with access limited to only authorized monitoring personnel and their supervising agents.

IT IS FURTHER ORDERED that the FBI, and any other law enforcement agency, is

permitted to intercept any electronic communications sent from, received by or occurring over the TARGET FACILITIES, including without limitation to any activity of any nature occurring within the TARGET FACILITIES, private messages and private chats sent from or received by the TARGET FACILITIES, draft private messages and private chats, and deleted private messages and private chats.

IT IS FURTHER ORDERED THAT the prosecutors or any other Special Assistant United States Attorney or Department of Justice Trial Attorney familiar with the facts of this case, shall cause to be provided to the Court a report on or about the fifteenth and thirtieth day following the date of the Order or the date interception begins, whichever is later, showing the progress that has been made toward achievement of the authorized objectives and the need for continued interception, although if the Order is renewed for a further period of interception, the application for renewal may serve as the report on or about the thirtieth day. If any of the above-ordered reports should become due on a weekend or holiday, such report shall become due on the next business day thereafter.


IT IS FURTHER ORDERED that this Order, as well as the supporting Application, Affidavit (along with its attachments), proposed Orders, and all interim reports filed with the Court, be sealed until further order of this Court, except that copies of the Order, in full or redacted form, may be served on the FBI as necessary to effectuate the Court's Order. Moreover, the United States may disclose the existence of the interception Order and the contents of pertinent intercepted communications, pursuant to Title 18, United States Code, Sections 2517(2) and (3), as appropriate for the purposes of providing relevant facts to a Court in support of any complaint, arrest warrant, and search or seizure warrant. In addition, the United States may disclose facts, pursuant to Title 18, United States Code, Sections

2517(2) and (3), to provide relevant testimony at any preliminary hearings, detention hearings, grand jury proceedings and other proceedings pertaining to the TARGET SUBJECTS and others as yet unknown. The United States may also disclose facts to foreign investigative or law enforcement officers, pursuant to Title 18, United States Code, Section 2517(7), as necessary to the proper performance of the official duties of the offer making or receiving such disclosure, and that foreign investigative or law enforcement officers may use or disclose such facts or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

IT IS FURTHER ORDERED that no inventory or return of the results of the foregoing interception need be made, other than the above required reports, before 90 days from the date of the expiration of the Order, or any extension of the Order, or at such time as the Court in its discretion may require; and

IT IS FURTHER ORDERED that, upon an ex parte showing of good cause to a judge of competent jurisdiction, the service of the above inventory or return may be postponed for a further reasonable period of time.

DATED: February 20, 2015



Anthony J. Trenga
~~HONORABLE JUDGE~~ ANTHONY J. TRENGA
UNITED STATES DISTRICT JUDGE

Presented by: AUSA Whitney Dougherty Russell
Trial Attorney Michael Grant